CLAIMS

1. Method to secure an electronic assembly implementing a calculation process characterised in that it consists in performing an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature.

2. Method according to claim 1, characterised in that it consists in performing at least once more all or part of the calculation in order to recalculate said signature and compare them in order to detect a possible error.

3. Method according to claim 1 or 2, characterised in that it consists in:
- performing an elementary operation using another "super-function" operation acting from and/or to a larger set;
- performing said calculation by said verification function using the result obtained by said super-function in order to obtain said calculation signature.

4. Method according to claim 3, characterised in that the calculation of the elementary operation can be found using the calculation of the super-function.

5. Method according to claim 3 or 4, characterised in that an elementary operation f of E in F is replaced by an operation f' of E' in F' where:
- E' and F' are super-sets of E and F;
- Move from E to E' by one-to-one function h_1;
- Move from F' to F by onto function h_2;
- for any element x of E we have: $h_2(f'(h_1(x))) = f(x)$.

6. Electronic assembly comprising storage means of a calculation process, processing means of said process, characterised in that it includes storage means of a verification function used to perform an additional calculation on intermediate results in order to obtain a calculation signature.

7. Computer program including program code instructions to execute the steps of the method according to one of claims 1 to 5 when said program is run in a computer system.

8. Smart card comprising storage means of a calculation process, processing means of said process, characterised in that it includes storage means of a verification function used to perform an additional calculation on intermediate results in order to obtain a calculation signature.

5